Privacy Guidelines for British Columbia Public Libraries

BRITISH COLUMBIA
Ministry of Education

Public Library Services Branch
May 2006

LEGISLATIVE LIBRARY OF BRITISH COLUMBIA
3 3298 00331 4771

Privacy Guidelines for British Columbia Public Libraries

British Columbia Public Library Services Branch
Ministry of Education

May 2006

VICTORIA BC JUN 30 2006

Library and Archives Canada Cataloguing in Publication Data
Main entry under title:
Privacy guidelines for British Columbia public libraries

Available also on the Internet.
Includes index.
ISBN 0-7726-5594-4

1. Public libraries - British Columbia - Administration. 2. Library records - Access control - British Columbia. 3. Confidential communications - Library records - British Columbia. 4. Public services (Libraries) -- British Columbia. 5. Privacy, Right of - British Columbia. 6. British Columbia. Freedom of Information and Protection of Privacy Act. I. British Columbia. Public Library Services Branch. II. British Columbia. Ministry of Education.

Z735.B88 P73 2006 025.1'974711 C2004-960149-6

2007-01352/

Table of Contents

1. Introduction 1

a) B.C. Libraries 1

b) Canada & B.C. laws protecting personal information 1

i) B.C.'s *FOIPPA* for public sector organizations 1

ii) B.C.'s *PIPA* for private organizations 2

iii) Canada's *Privacy Act* for government institutions 2

iv) Canada's *PIPEDA* for private organizations 2

c) Purpose of Guidelines 2

d) How to use the Guidelines 3

i) "She", "her" or "herself" 3

ii) References within the Guidelines 3

iii) Definitions 3

2. Registration 4

a) Collecting personal information 4

i) Only collect personal information that is required 4

ii) Only by trained employees and volunteers 5

iii) Best practices re patron ID 5

iv) On-line registration 5

v) Collecting ID numbers and references for debt collection 5

vi) Recording other family members' personal information 6

b) Information individuals need to know when personal information is collected 6

i) When registering using on-line or paper registration forms 6

ii) When registration information is input directly into the system 7

iii) Privacy policies & procedures 7

c) Children 7

i) Collecting children's personal information 8

ii) Parent/guardian authorization 8

d) Home service 8

e) Non-residents 9

f) Personal information for marketing or fundraising 9

3. Circulation 10

a) Only authorize employees & volunteers who need access 10

b) Computer screens 10

c) Receipts showing materials borrowed 10

d) Sharing information with friends or family 11

e) Family or friends using another patron's card 11

f) History of what a patron borrowed 12

i) Parent's access to child's borrowing history 12

ii) Home Service patrons' borrowing history 13

g) History of who borrowed an item 13
h) Books on hold 13
i) Home Service 14
j) Paper book cards 14
k) Patron cards held by library 14
l) Unreturned materials 14
i) Automatic overdue notification 15
ii) Retention of information 15
iii) Children 15
iv) Collection agencies 15
v) Communication with other libraries 16
m) Faxing or emailing personal information 16
n) RFID (Radio Frequency Identification) 17

4. On-line Services 17

a) Registration on-line 17
b) On-line reference questions 17
c) Outside databases 18

5. Internet/Computer Access 18

a) Notice 18
b) Logs, sign-up sheets & registration forms 19
i) Log of users 19
ii) Sign-up sheets 20
iii) Computer use registration forms 20
iv) Destroying logs, sign-up sheets and registration forms 20
c) History log 20
d) Back-ups 21
e) Surveillance of computer area 21

6. Reference Questions 21

a) In person 21
b) Electronically 22
i) Emailed to library 22
ii) On-line to the library through its own website 22
iii) On-line through an outside service provider 23
c) Questions referred to other libraries or resources 23

7. Employee & Volunteer Personal Information 24

a) Surveillance 24
b) Work contact information 24
c) Pseudonyms 24

8. Personal Information Access & Correction 25

a) Access to routine information 25
b) Access to non-routine information 25
c) Correction of personal information 25

d) Children 25
e) Others (employees, volunteers, donors) 26

9. Disclosure of Personal Information 26

a) Family & friends 26
b) Police 26
c) Social workers and school counsellors 27
d) Collection agencies 27
e) Other libraries 27

10. Records Retention & Disposal 28

a) In general 28
b) Back-ups 29
c) Borrowing history 29
d) Book/resource history 29

11. Outside Service Providers 29

a) Services provided on behalf of the library 29
b) Referrals to services or organizations outside the library 30
i) On-line services 30
ii) Collection agencies 30
c) Janitorial or other services 31

12. Security 31

a) Authorized employees and volunteers 31
b) Confidentiality agreements 31
c) Training 31
d) Technology 32
e) Physical security 32
f) Surveillance 33

13. Miscellaneous 33

a) Disclosure, storage or access outside Canada 33
b) Library system changes 34
c) Objectionable behaviour of patrons 34
d) Room rentals 35
e) Donor personal information 35
f) Research 35

14. Policies & Procedures 36

a) Privacy policies 36
i) General 37
ii) Website 37
b) Procedures – Instructions to employees & volunteers 37
i) Training 37
ii) Communication of policies to patrons 37

iii) FOI/Privacy Officer ____ 37
c) Personal Information Directory (PID) ____ *38*
d) Privacy Impact Assessment (PIA) ____ *38*

Appendix I – Additional Resources ____ ***39***

a) Legislation ____ *39*
b) Helpful contact information ____ *39*
c) Helpful documents ____ *40*

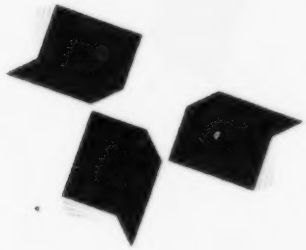
Appendix II – Sample Privacy Clauses ____ ***41***

a) Authority to collect personal information ____ *41*
b) Registration form ____ *41*
c) Un-secure communication from website ____ *41*

Appendix III – Sample Website Privacy Policy ____ ***42***

Appendix IV – Sample General Privacy Policy ____ ***46***

Index ____ ***51***



1. Introduction

Public libraries in British Columbia fall under the definition of "local public bodies" under the *Freedom of Information and Protection of Privacy Act (FOIPPA)*. As such, libraries are responsible for protecting personal information in accordance with the provisions of *FOIPPA*.

a) B.C. Libraries

Public libraries are an important resource for individuals in B.C. They provide open and equitable access to valuable information and resources. As information technologies continue to emerge, B.C. public libraries strive to use them to the best advantage of the public.

Privacy has long been a concern for many individuals, including librarians. As information technology expands, concerns over individual privacy also grow, particularly those relating to how individuals' personal information is protected.

b) Canada & B.C. laws protecting personal information

The governments of Canada and B.C. (as well as other provinces) have written laws to protect personal information in the care of both public and private organizations. The following is a brief summary of the federal and B.C. legislation currently in place:

i) B.C.'s FOIPPA for public sector organizations

B.C.'s *Freedom of Information and Protection of Privacy Act* (*FOIPPA*) protects personal information collected, used or disclosed by "public bodies" in B.C. Public bodies include government ministries; Crown

corporations; agencies, commissions & boards; municipalities; municipal police; public hospitals, schools, universities and colleges; and public libraries.

The privacy protection part of *FOIPPA* sets out the minimum requirements for how public bodies must protect personal information (Act, Part 3). There is also an important "access to information" aspect of *FOIPPA* that allows individuals and organizations access to other non-personal information held by public bodies (Act, Part 2).

See how to access FOIPPA in Appendix I.

ii) B.C.'s PIPA *for private organizations*

B.C. is one of the first provinces to provide legislation protecting personal information collected, used or disclosed by "private organizations." The *Personal Information Protection Act* (*PIPA*) applies to all organizations in B.C., such as businesses, associations, unions, and non-profits.

See how to access PIPA in Appendix I.

iii) Canada's Privacy Act *for government institutions*

Canada's *Privacy Act* protects personal information collected, used or disclosed by federal government institutions. Government institutions are listed in the Schedule to the *Privacy Act* and include Library and Archives Canada.

See how to access the Privacy Act in Appendix I.

iv) Canada's PIPEDA *for private organizations*

Canada's *Personal Information Protection and Electronic Documents Act (PIPEDA)* protects personal information collected, used or disclosed in the course of commercial activities by federally regulated organizations (e.g. banks), all private organizations across Canada (except where a province has substantially similar legislation, such as B.C. Alberta and Quebec), or where it is communicated across a provincial or international border.

See how to access PIPEDA in Appendix I.

c) Purpose of Guidelines

These Guidelines provide information to public libraries and do not constitute legal advice. As a public body under *FOIPPA*, each public library is responsible for its own compliance with *FOIPPA* and should use its own judgment in making decisions with respect to its compliance. Libraries should consider the privacy protection requirements in *FOIPPA* merely as

minimum standards required. Any amendments that may be made to *FOIPPA* after May 2006 have not been anticipated nor are they reflected in the Guidelines.

d) How to use the Guidelines

i) "She", "her" or "herself"

Wherever the feminine gender is used, it should be read as both feminine and masculine (i.e. as "she/he", "her/him", or "her/himself").

ii) References within the Guidelines

References are made throughout the Guidelines to different sections of *FOIPPA* and its Regulation. References to *FOIPPA* will appear as "(Act, s. #)"; references to the Regulation will be cited as "(Reg., s. #)".

Cross references to other relevant areas in the Guidelines are provided at the bottom of many sections. Additional resources are provided in Appendix I. An index is also available at the back of the Guidelines.

iii) Definitions

There are some terms that are commonly used in the area of personal information protection. It may be helpful to read over the more common ones in Box 1.1 below. The terms below are italicized when used in the Guidelines, with the exception of "personal information" because of how often it is used.

Box 1.1

Definitions for common terms used in these Guidelines:

- *Personal information* → recorded information about an identifiable individual other than work *contact information* (see below), such as name, home address, identification numbers (including barcodes), birth date, and reading choices (Act, Schedule 1).
- *Contact information* → information you would often find on a business card that allows a person to be contacted at a place of business, such as the name, title, business telephone number, business address, business email, or business fax number of the individual (Act, Schedule 1).
- *Record* → includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records (Act, Schedule 1).
- *FOI/Privacy Officer* → the library employee who is responsible for the library's compliance with *FOIPPA* (Act, s. 77).

2. Registration

B.C. public libraries are as diverse as the communities they serve. Registration systems often reflect these diversities.

Depending on the library, registration of a new patron may be done by means of a paper registration form, direct entry into the library's computer system, on-line application, verification and transfer of information from an on-line application, or a combination of these.

Regardless of the registration system, libraries must carefully consider the personal information they collect and how it is handled (Act, Part 3).

a) Collecting personal information

Public libraries are authorized to collect personal information under the *Library Act* and section 26 of *FOIPPA*. Collection occurs in a variety of ways and for several purposes. Below are some of the considerations when collecting personal information during the registration process.

See "Circulation", "Internet/Computer Access", "Reference Questions", and "Outside Service Providers" for more information about collecting personal information.

i) Only collect personal information that is required

Libraries may only collect personal information that is necessary for the library to offer its services and operate its programs or otherwise authorized by *FOIPPA* (Act, s. 26). For example, if knowing the first language of a patron is not necessary, it should not be collected.

When libraries wish to collect information for statistical purposes or to learn more about their patrons for the purpose of planning or managing their programs and services (such as reading preferences and preferred language), separate forms should be used with no personal identifiers.

Once the statistical information is compiled, the original forms should be shredded.

Box 2.1

NOTE for Smaller Communities:

In smaller communities, information collected anonymously could still identify an individual. For example, there may be only one man in town who is over 70 and whose preferred language is Hungarian. Because the individual may be identified, this is still personal information and needs to be protected as such.

See "Information individuals need to know when personal information is collected", below.

ii) Only by trained employees and volunteers

Only employees and volunteers who are fully aware of the requirements for protecting personal information should be authorized to collect personal information.

iii) Best practices re patron ID

Most libraries require individuals to provide identification showing their name and home address. It is best not to record the ID number. If a library wants to document that ID was checked, a check box on the paper form or a flag in the computer system is sufficient. It may be helpful, especially for new employees and volunteers, to avoid providing any space on the form that may look like it is intended for recording an ID number.

Some libraries allow patrons to borrow expensive reference materials for a short period of time if the patron leaves something of value, such as their keys or a piece of ID. It is preferable from a privacy perspective not to keep an ID card or anything else with personal information.

See "Collecting ID numbers and references for debt collection" (below) and "Reference Questions: In person" for more information.

iv) On-line registration

Libraries that allow patrons to register on-line should ensure that the personal information is protected during the communication process (e.g. using 128-bit encryption technology).

If the communication is not secure, libraries should state this very clearly to individuals who may wish to register on-line.

Personal identification numbers (PINs) issued should be randomly chosen. Non-random numbers, such as the last 4 digits of an individual's phone number or birth date may be easily guessed by a third party.

v) Collecting ID numbers and references for debt collection

Libraries that have difficulties with unreturned resources may wish to collect certain personal information (such as ID numbers or references) specifically for the purpose of debt collection (see Box 2.2 below). Where an individual's personal information is collected specifically for the purpose of debt collection, libraries must inform the individual of this at the time the information is collected (Act, s. 27).

Cont'd...

Box 2.2

TIPS for collecting ID numbers and references:

- Before collecting ID numbers for debt collection purposes, make sure the library or the collection agency has legal authority to use the ID numbers in collecting debts. For example, can they legally use certain ID numbers to find the patron's current address?
- When collecting personal references (e.g. contact information for a patron's parents or friends), be careful to only collect
  - work *contact information* (name, business phone number and address), or
  - information that is listed in the local telephone directory,
  - unless the reference person has provided consent for the collection (Act, s. 27(1)).

vi) Recording other family members' personal information

Personal information about another member of a patron's family should not be collected without the family member's consent (Act, s. 27(1)).

See "Children" below for information about children's registration.

b) Information individuals need to know when personal information is collected

Any time personal information is collected from an individual, employees or volunteers must give her information about

- the purpose(s) for collecting it,
- the legal authority for collecting it, and
- the person she can contact for more information and their contact information (including the person's title, business address and phone number) (Act, s. 27(2)). (See Box 2.3 below).

Box 2.3

FOI/Privacy Officer

A library must have a designated employee responsible for the library's compliance with *FOIPPA* (Act, s. 77(a)) . In these Guidelines, this person will be referred to as the library's *FOI/Privacy Officer*.

i) When registering using on-line or paper registration forms

Registration forms (paper or on-line) are an excellent place to include a statement that communicates the required information to individuals when their personal information is collected (see (b) above); they can also direct individuals to the library's privacy policies for more information.

Paper forms with personal information should be shredded when no longer needed.

See "Records Retention & Disposal" and "Appendix II: Sample Privacy Clauses" for more information.

ii) When registration information is input directly into the system

When a patron's information is entered directly into the library's computer system, the employee or volunteer entering the information should communicate the above required information (under (b) above) to the new patron. This can be done by calling the individual's attention to a notice on the registration desk that sets out the information or by giving the individual a brochure with the library's privacy policies, which includes this information.

See the "Appendix II: Sample Privacy Clauses".

iii) Privacy policies & procedures

Libraries should have privacy policies setting out their personal information protection practices. These policies must be made readily available to the public (Act, s. 70).

Libraries should also have clear procedures to guide employees and volunteers in the handling of personal information in different situations they may encounter in the library. These procedures must be made readily available to the public (Act, s. 70).

Box 2.4

Good places for letting patrons know about privacy policies and procedures:

- Library cards are great places for brief privacy statements and to refer patrons to the library's privacy policies and procedures for more information.
- Notices at Registration and Circulation counters provide good places to let patrons know where they can read the library's privacy policies.
- The Library's website can provide full privacy policies and procedures.

See "Appendix II: Sample Privacy Clauses" and "Appendix IV: Sample General Privacy Policy".

c) Children

Many library patrons are children. This section deals specifically with children's registration.

See other sections regarding children's personal information under "Circulation: History of what a patron borrowed", "Circulation: Unreturned materials", and "Personal information access & correction".

i) Collecting children's personal information

Libraries are authorized to collect personal information from children in order to register them for library services (*Library Act* and Act, s. 26). Only personal information that is required for membership should be collected.

See "Collecting Personal Information: Only personal information required" above for more information.

ii) Parent/guardian authorization

Libraries generally have policies requiring that children under a certain age have their parents or guardians authorize their membership applications. In most cases, the adult signs an agreement to be responsible for the materials borrowed by the minor child. This allows the library to contact the parent/guardian regarding overdue books and fines.

Where this is the case, children 12 years old and over should be told that the library may disclose personal information to the parent/guardian, such as book/resource title, where necessary to recover overdue materials. This notification could be provided on the registration form.

Box 2.5

Why should children be given this notice?

- Children have the right to control the disclosure of their own personal information (and to access or correct it). It is only when a child is "incapable" of exercising her rights that a parent or guardian may do so on her behalf (Reg., s. 3).
- While the *FOIPPA* Regulation does not specify an age at which a child is deemed to be "capable" of exercising her own information rights, section 76 of the *Child, Family and Community Service Act* establishes 12 as the age at which a child in care may exercise her own access, disclosure and correction rights. This provides a useful guideline for establishing an age in policy.
- However, libraries should keep in mind that a child under 12 who is "capable" of exercising her own information rights has the right to do so. Policies should not be applied so rigidly that such a child is not able to exercise her rights under *FOIPPA*.

See "Circulation: Unreturned materials: Children", "Personal information access & correction: Children", and "Appendix II: Sample Privacy Clauses" for more information.

d) Home service

Some libraries offer home service for patrons who have special needs. Additional personal information may be required in order to offer these services. For example, if library employees or volunteers choose the resources, they may need to know the patron's reading preferences, whether large print or audio books are needed, emergency health and contact information, and what the patron has already borrowed to avoid duplication.

Where a service cannot be provided unless a patron provides evidence of a documented disability (e.g. Talking Books), libraries should not photocopy the evidence/certificate, unless absolutely necessary for a specified purpose. Instead, a note should be made of the fact that the appropriate certificate was shown and any other necessary information, such as an expiry date.

Only the personal information required to offer the services should be collected (Act, s. 26). Extra care should be taken to ensure that any sensitive health information collected is securely stored.

See "Security" and "Circulation: Home Service" for more information.

e) Non-residents

Libraries sometimes allow visitors and other non-residents limited and/or temporary membership privileges. There may be a real concern for libraries over collecting unreturned material. In such cases, libraries may want individuals to provide a credit card number as security. If the library is able to charge to the credit card for the overdue materials, then collecting the credit card information may be reasonable. The individual must be informed that the credit card number is being collected for this purpose. Extra care should be taken to ensure that credit card numbers are securely stored.

Also see "Security".

f) Personal information for marketing or fundraising

Personal information should not be disclosed for marketing or fundraising purposes unless the patron's consent is obtained. Consent can be obtained easily by providing a box on application/registration forms patrons can check to either "opt-in" or "opt-out" of being contacted for marketing or fundraising purposes.

Box 2.6

"Opt-in" vs. "Opt-out" by ticking a box on a form:

- *"Opt-out"* → a box is provided for an individual to indicate that she does not consent. If the individual filled-in the form but did not tick the "opt-out" box, she is considered to have consented.
  - This type of consent should not be used where sensitive personal information is involved.
- *"Opt-in"* → a box is provided for an individual to tick if she wishes to consent.
  - This is the higher level of consent, because it requires the individual to actively choose to consent.

3. Circulation

a) Only authorize employees & volunteers who need access

Libraries should limit employee and volunteer access to personal information to only those who need access to the particular type of information in order to perform their job functions. Rooms, filing cabinets and databases containing personal information should only be accessible to those employees or volunteers.

See "Security" for more information.

Box 3.1

Examples of restricting access on a need-to-know basis:

- *Patron name, barcode, contact information* → only employees or volunteers who check out materials, update personal information or place holds for patrons (e.g. Circulation and Reference staff).
- *Patron borrowing history* → only employees or volunteers who assist patrons to access this information (employees and volunteers should be discreet and avoid looking at the information themselves where possible).
- *Home Service patron's disability information, reading preferences, and borrowing history* → only employees & volunteers who make selections for Home Service patrons & update their personal information.
- *Employee timesheets* → only employees or volunteers responsible for supervising employees & volunteers or payroll.
- *Employee criminal record check reports* → only employees or volunteers responsible for screening employees in this regard (e.g. Human Resources Director, Chief Librarian or Board members).

b) Computer screens

Employees and volunteers should take care when personal information is visible on a computer screen. The screen should not be visible to unauthorized persons, such as other patrons or employees/volunteers, who do not need access to personal information.

c) Receipts showing materials borrowed

Receipts provided to patrons showing what they have borrowed should not show personal information. Member *barcodes* are unique identifiers and therefore personal information.

If *barcodes* appear at all on the receipt, they should show only the last 4 digits (e.g. **********1423). In addition to protecting personal information, this will allow patrons who use the receipts to keep track of family library loans by individual member to continue doing so.

Box 3.2

Is blocking out *barcode* numbers on receipts really necessary?

- Many individuals are becoming more and more sensitive to protecting their personal information and may object to their *barcodes* appearing on receipts (retail store systems are being updated to blank out credit card numbers on receipts).
- While receipts are given directly to patrons, they may be lost or left out where others can access them.
- Someone may be able to access personal information about an individual, such as reading history, with the individual's *barcode*.
- Where libraries do not have control over whether or not *barcodes* appears on receipts, they should ask their vendor to add this functionality.

d) Sharing information with friends or family

Libraries must not share a patron's personal information with the patron's friends or family members without her consent, unless authorized by *FOIPPA* (Act, s. 33) (see Box 3.3 below for examples).

Personal information about a patron should also not be given out over the phone without the patron's consent, even if the caller provides the patron's *barcode* number (the *barcode* is not enough to prove consent, as the card may have been stolen).

Consent must be provided in writing, specifying to whom the personal information may be disclosed and how it may be used (Act, s. 33.1(1)(b) & Reg., s. 6).

Box 3.3

Examples of when a library may disclose a patron's personal information to the patron's friend/family:

- To collect a debt owed by the individual the personal information is about,
- where the library believes there are "compelling circumstances...that affect anyone's health or safety", or
- so that a person's next of kin or friend can be contacted to let them know that the person is injured, ill or dead.

In all cases, only the minimum information needed should be disclosed.

See sections 33.1 and 33.2 of the Act for a complete list of exceptions.

See "Disclosure of personal information: Family and friends" for more information.

e) Family or friends using another patron's card

Libraries should not allow a patron's family or friends to sign out an item with the patron's library card, unless the library has consent from the patron.

A patron must provide consent in writing, specifying to whom the personal information may be disclosed and how it may be used (Act, s. 33.1(1)(b) &

Reg., s. 6). For example, a patron may give written consent for her sister, Mary Ann, to pick up materials on her behalf, solely for the purpose of delivering the materials to the patron. If consent is given for ongoing pick-up of materials, a library may wish to make a note on the patron's file.

See "Sharing information with other family members" above for more information.

f) History of what a patron borrowed

Libraries should not keep a history of what materials a patron has borrowed, except where the individual consents. Once an item has been safely returned, reference to it should be removed from the patron's record.

For some patrons, having a record of what they have borrowed (or searched for) is a valuable reference. However, borrowing history can also disclose sensitive personal information about an individual, such as certain personal preferences and health concerns. If libraries wish to offer this service, it should be available on an "opt-in" basis (i.e. must be expressly requested – see Box 2.6). Patrons should also be able to stop recording their borrowing history (and to purge the old record).

Box 3.4

What about existing systems that do not allow any flexibility?

- Some libraries' computer systems do not provide the ability to choose whether a patron's reading history is recorded, nor to turn it off or purge the previously recorded information.
- This should be disclosed to patrons through the library's privacy policies.
- Any new system should offer patrons the ability to make choices with respect to any recording of their reading histories.

i) Parent's access to child's borrowing history

Libraries sometimes have policies allowing parents or guardians to view the borrowing history of their children under a certain age. Where there is such a policy, it should set the age at under 12 years.

If a child under 12 years old objects to her parent accessing information about her borrowing history (or any other personal information), or if a child is over 12, the parent or guardian's request should be referred to the library's *FOI/Privacy Officer*. This can be a complex area and the FOI/Privacy Officer is in the best position to determine what access is appropriate.

See "Personal information access & correction" for more information.

ii) Home Service patrons' borrowing history

Home service is one example of where it may be necessary to keep track of what patrons have borrowed in order to avoid selecting resources the patron has already borrowed.

See "Registration: Home Service", and "Home Service" below, for more information.

g) History of who borrowed an item

A patron's personal information should only be recorded in association with a borrowed item until the record is no longer necessary. For example, if a record of the last borrower is necessary to ensure that resources are returned undamaged and library employees or volunteers are able to check the condition of books as they are checked in, the record of the last borrower's personal information should be removed at that time.

If a library's current system is not able to purge personal information right away, this should be communicated in the library's privacy policies. Appropriate privacy protection measures should be included in any new system.

See "Miscellaneous: Library system changes" for more information.

h) Books on hold

Some libraries display books on hold in common areas for patrons to pick up. This potentially allows other individuals to access the materials and identify patrons' reading choices. Where it is not feasible to offer this service without leaving the books in common areas, steps should be taken to protect the patron's privacy.

Box 3.5

Steps to protect patron privacy for books on hold in common areas:

1. Individuals should be advised before they place an item on hold that it will be available for pick up in a common area,
2. a minimum of personal information should appear on the outside of the book to identify who the material is for, and
3. the spine of the book or other resource should be covered (e.g. paper folded around spine with patron's first initial and last name secured with elastic band).

No one other than the patron herself should be permitted to pick-up an item on hold, unless the library has the patron's consent.

See "Sharing information with friends or family" and "Family or friends using another patron's card" above for more information.

i) Home Service

Patrons receiving Home Service usually provide more personal information than is collected from other patrons. This often includes information regarding what the patron's needs to accommodate her disability, reading preferences, and reading history. Only employees and volunteers who work directly in the Home Service program and who need access to the home service patron information should have access to it.

See "Security" and "Registration: Home Service" for more information.

j) Paper book cards

Some libraries use paper book cards to keep track of borrowed materials. Book cards listing each patron who has borrowed the material disclose patrons' personal selections to others who may see the card later. Where no other system for recording circulation materials is feasible, patrons should be given the option, on an individual basis, of having their reading selections recorded privately.

Box 3.6

Privacy enhancing ideas for libraries that use paper book cards:

- Keep paper books cards at the Circulation Desk and have employees or volunteers write the patron's name.
- Low-tech automation: Use a simple database or spreadsheet to record the patrons' names beside the ISBN, call number and/or title of the resources out on loan.

k) Patron cards held by library

Libraries that keep patron cards in the library should not allow patrons to find their own cards from among those of other patrons (Act, s. 33). Instead, employees or volunteers with authority to access personal information of patrons should give the cards out. If the employee or volunteer does not know the patron, she should ask to see identification to make sure that the card is being given to the right person.

l) Unreturned materials

Libraries use a variety of methods to collect unreturned materials. Libraries may disclose personal information without consent for the purpose of collecting a debt owed to them (Act, s. 33.1(1)(i)). However, disclosure should be limited to personal information that is reasonably necessary to collect the debt.

i) Automatic overdue notification

Libraries should let patrons know if they use automatic overdue notices that are not private, such as automatic telephone messages and postcards. An appropriate place for such a notice may be the library's privacy policies.

ii) Retention of information

Personal information about patrons who have not returned materials should be kept only as long as is necessary, such as when it is necessary to enforce library rules or to collect on a debt.

For example, there are legal limits on how long an organization may take legal action to recover on a debt. And, the *Library Act* (s. 47(c)) allows libraries to exclude an individual in certain circumstances. It may therefore be reasonable to keep personal information until the library is no longer able to collect on the debt or for as long as the library is able to exclude the individual under the *Library Act*.

See "Records retention & disposal" for more information.

iii) Children

If a child has not returned a borrowed item, the library may disclose the child's personal information in order to collect the debt (Act, s. 33.1(1)(i)). Where a parent or guardian has agreed to be responsible for materials borrowed by the child, her personal information may also be disclosed for this purpose. In either case, disclosure should be limited to what is reasonably necessary to collect the debt.

Box 3.7

Example → Maber's mother signed his library card application, agreeing to be responsible for what he borrows. The library may call her to ask for the overdue book to be returned. In doing so, the library may describe the unreturned book to Maber's mother. If the book is still not returned and the library has not been able to collect the fine owing, it may give a collection agency personal information about Maber's mother's that is reasonably necessary to collect the debt.

See "Registration: Children", "Personal information access and correction", and "Collection agencies" (below) for more information.

iv) Collection agencies

A library may want to use a collection agency to collect a debt. Personal information may be disclosed to a collection agency for this purpose without consent from the individual to whom it belongs. Only personal information reasonably needed by the collection agency should be provided. The personal information must not be disclosed outside

Canada unless it is reasonable to believe that the person who owes the debt lives or has assets in another country (Act, s. 33.1(1)(i)).

See "Collection agencies" under "Registration: Collecting personal information: Collecting ID numbers and references for debt collection", "Outside service providers: Referrals to services or organizations outside the library", and "Disclosure of personal information".

v) Communication with other libraries

A library may ask other libraries for personal information about a patron for the purpose of collecting a debt owed by that individual as a result of not returning a library resource (s. 27(1)(b) & 33.1(1)(i)).

Personal information collected and/or disclosed should be limited to what is reasonably necessary to collect the debt owing. This is normally limited to information needed to locate the individual.

Libraries should not share "black lists" or share patron personal information in a general way (e.g. not specific to a debt) during meetings or discussions.

See "Collection agencies" (above) and "Disclosure of personal information: Other libraries" for more information.

m) Faxing or emailing personal information

Library employees and volunteers should take care when faxing or emailing personal information. Sensitive personal information, such as financial or health information should not be faxed or emailed unless it must be received immediately and faxing or emailing is the only way to do so. Even where the personal information is not sensitive, cautionary steps should be taken to ensure that the information only reaches the intended recipient. If faxing personal information is an ongoing, routine or an integral part of the library's operations, encryption or other secure transmission techniques should be used.

Box 3.8

TIPS for faxing or emailing personal information:

- Fax machines that send or receive personal information should be in secure areas.
- When sending personal information by fax, use a cover sheet with the name of the recipient and the number of pages.
- Include a confidentiality clause on the fax cover sheet or in the email. Check that the number dialled or the email address used is correct prior to sending the personal information.
- Once a fax is sent, check the confirmation report to ensure that it was sent to the intended number.
- If it is necessary to fax or email sensitive personal information, call ahead to confirm the fax number or email address and the appropriate person to receive the fax/email. Ask the person to wait for the fax/email and call to confirm when she has received it.

See the Office of the Information & Privacy Commissioner's Guidelines on "Faxing and Emailing Personal Information" for more information, on-line at http://oipc.bc.ca/pdfs/public/fax-emailguidelines(Feb2005).pdf.

n) RFID (Radio Frequency Identification)

Libraries wishing to explore implementing RFID technology should carefully examine the privacy implications of this technology. Privacy requirements should be incorporated into any Request for Quotation (RFQ) or Request for Proposal (RFP) concerning potential RFID technology. Additionally, a Privacy Impact Assessment (PIA) should be conducted early in the design phase and completed prior to the implementation of RFID technology in the library system.

See the Office of the Information and Privacy Commissioner of Ontario's "Guidelines for Using RFID Tags in Ontario Public Libraries" online at http://www.ipc.on.ca/docs/rfidgdlines.pdf for information in the context of privacy protection in that province. Also see "Policies & procedures: Privacy Impact Assessment (PIA)" in these Guidelines for more information.

4. On-line Services

Libraries should develop privacy policies for their websites that relate directly to personal information collected that is used, retained and/or disclosed in the course of visiting and/or navigating through the site. These policies must be made readily available to the public (Act, s. 70).

See "Policies & procedures" and "Appendix IV: Sample General Privacy Policy" for more information.

a) Registration on-line

Registration on-line should be over a secure connection (e.g. using 128-bit encryption). If not, a notice should clearly state to anyone using the service that any information they send is not secure and may be accessed by others. Individuals should also be informed that other more secure methods of registration are also available (such as registering in person). Libraries assigning personal identification numbers (PINs) should use random numbers (not non-random numbers, such as the last 4 digits of a phone number).

Also see "Registration: Collecting personal information: On-line registration".

b) On-line reference questions

Reference questions are sometimes emailed to a library. Some libraries may provide a chat-like system on-line to answer reference questions. In either case, if personal information is collected (such as IP address, email address, or name), the individual must be informed of the purpose for collecting the

information, the library's legal authority for collecting it, and information about how to contact the library's *FOI/Privacy Officer* (Act, s. 27).

See "Reference Questions: Electronically" for more information.

c) Outside databases

Libraries often provide access to services offered by other organizations and hosted on the organizations' own websites (e.g. EBSCO). When a link takes a visitor from the library's website to that of another organization, clear notice should be provided beside the link that lets the individual know she is about to leave the library's website and visit the site of another organization. It should also recommend that she check their privacy policies.

Box 4.1

Going the extra mile:

When considering whether to offer a link from your site to that of another organization:

- Check the organization's privacy policies to see if they comply with *FOIPPA*.
- If they do not, try to negotiate for an increase to their privacy policies to comply with *FOIPPA*.
- At minimum, try to negotiate for their privacy policies to disclose specifically the purpose of collecting personal information, how it is used, to whom it is disclosed, and the contact information for someone who can provide more information about their personal information protection practices.

See "Reference Questions: Electronically: On-line though an outside provider" and "Outside service providers: Referrals to services or organizations outside the library" for more information.

5. Internet/Computer Access

a) Notice

Libraries must provide a notice to individuals with access to library computers if any personal information is collected (even if only web-browsing information is stored, as long as it could be somehow associated with the individual). At minimum, the notice must state the purpose for collecting the information, the library's legal authority for collecting it, and information about how to contact the library's *FOI/Privacy Officer* (Act, s. 27). It should be placed where it can be easily noticed and where the individual can read it before using the computer.

Box 5.1

Examples of things to consider when writing a notice:

- Are the URLs of websites that are visited stored in the computer's cache or history folder? If so,
  - is the cache or history purged when the person logs out? (Do they have to ensure they log-off themselves?)
  - is an electronic or paper log kept of individuals who have used a particular computer that can be cross-referenced with the cache or history folder?
  - is there surveillance of the computer area allowing the video record to be cross-referenced with the cache or history folder?
- If personal information is collected by means of a log of individuals using a computer, or surveillance records, the library must provide the following information:
  - the purpose for its collection,
  - the library's legal authority for collecting it (see "*Appendix II: Sample Privacy Clauses*")
  - the contact information for the library's *FOI/Privacy Officer* (Act, s. 27)
- How long is the personal information kept (e.g. minimum of one year if used to make a decision affecting the individual) (Act, s. 31)?
- Are internet transactions secured so that individuals may feel confident about using the internet for confidential communications?
- Where the library provides wireless internet access, is the connection secure so that individuals may feel confident about confidential communications?
- Does the computer allow individuals to save preferences (including usernames and passwords) that could later be accessed by someone else?
- Are there rules for using the computer/internet that encourage respect for the privacy of others (e.g. not looking at other's monitor)?
- How can individuals contact the person responsible for the library's compliance with *FOIPPA* if they have any questions?

b) Logs, sign-up sheets & registration forms

Personal information may only be collected where it is necessary for a library's programs or services (or another purpose authorized by *FOIPPA*, see Act, s. 26). Libraries often keep track of computer use in some way. Some libraries create logs to enforce library computer use policies. Others only use sign-up sheets to allow individuals to book computer space.

i) Log of users

Libraries that keep track of computer use to enforce library computer policies, such as maximum time and appropriate use, must keep the logs for a minimum of one year so that an individual can access her personal information (Act., s. 31(b)) .

ii) Sign-up sheets

Libraries using sign-up sheets merely to allow individuals to book computer time (not to enforce library policies) should destroy the sign-up sheets as soon as possible. For example, some libraries keep statistical records of computer access; the sign-up sheets should only be kept until the statistical data has been collected.

Box 5.2

TIPS for privacy friendly sign-up sheets:

- Let individuals know what authorizes the library to collect personal information, what any personal information on the sign-up sheet is used for, and how they can contact the library's *FOI/Privacy Officer* (Act, s. 27).
- Include recording statistical data and shredding the sign-up sheets in the library's daily closing procedures.
- Keep in mind that any information that is about an identifiable person is personal information. So even if the sign-up sheet is full of common first names and pseudonyms, treat it as personal information.

iii) Computer use registration forms

Some libraries require individuals to sign a registration form prior to being allowed access to computers. These must be kept for a minimum of one year, to allow the individual the opportunity to access the personal information on the form (Act., s. 31(b)).

iv) Destroying logs, sign-up sheets and registration forms

When destroying logs, sign-up sheets or registration forms containing personal information, a method should be used that is appropriate for the media. For example, paper logs should be shredded and data in computer drives should dealt with in a way that does not allow its recovery (do not merely delete files).

See "Records retention and disposal" for more information.

c) History log

Libraries should purge the cache and history folders in computers that are used by individuals as often as is practicable.

Box 5.3

Examples of when to purge personal information from computers:

- *If individuals must log-on to use the system* → purge personal information (including cache/history) upon log-off. Arrange for automatic log-off after a certain period if an individual does not log-off herself.
- *If the computer may be used without logging on* → set up a routine to purge personal information (including cache/history) each night, or when the computer is turned off (ideally, at the end of each day).

d) Back-ups

When destroying computer data, libraries should consider whether the information is retained elsewhere as a result of a backup procedure. If so, the data on the backup should be destroyed also.

See "Records retention & disposal" for more information.

e) Surveillance of computer area

Surveillance (Close Circuit TV or any other audio/visual recording device) should be used only as a last resort.

Personal information is being collected if there is recorded surveillance of individuals using computers (e.g. their image and actions). If a recording of an individual is used to make a decision that affects her, such as suspending her privileges, the library must keep the recording of that personal information for at least one year, so she can access it (Act., s. 31(b)).

See "Security: Surveillance" for more information.

6. Reference Questions

Public libraries provide a valuable service in helping individuals to find information. This is accomplished in a variety of ways, including in person in the library, by email, through the library's own website, or through a third party service provider. Questions are also sometimes referred to other libraries or resources.

a) In person

Often questions are answered without library employees or volunteers writing down any personal information. If it is, the library should remove and destroy the personal information or destroy the whole record as soon as is practicable.

Many libraries keep track of questions for follow up, in case they are asked again, or to compile statistical information. Personal information should be removed whenever possible. For example, write the individual's name on the top of the paper; tear that part of the paper off and shred it once the question is answered.

Cont'd...

Box 6.1

Patrons borrowing expensive reference materials :

- Some libraries allow patrons to borrow expensive reference materials for a short period of time if the patron leaves something of value, such as their keys or a piece of identification (such as a Driver's License).
- Where possible, it is preferable from a privacy perspective not to use ID or anything else with personal information.
- If there are no other reasons (legal or otherwise) why an ID card should not be kept while the item is borrowed, and a library chooses to keep an ID card, extra care should be taken to ensure that the card is secure.

See also "Registration: Collecting personal information: Best practices re patron ID".

b) Electronically

i) Emailed to library

Questions emailed to the library include an email address, which may be personal information (e.g. if it is an individual's personal email address). An individual's personal information should not be kept once a question has been answered, unless necessary for a specific purpose. Examples of where it may be necessary include the following: further related questions are anticipated from the individual, there are specific legal reasons to keep it, or the information has been used in a decision that affects the individual (in which case, it must be kept for at least one year).

Box 6.2

QUICK TIPS:

- Cut & paste emailed questions into a spreadsheet, word processing document or database, without the personal information.
- If you include the answers as well, you could have the beginning of a FAQ resource.

ii) On-line to the library through its own website

Libraries using the internet to answer reference questions sometimes do so through a form on their website, that emails directly to the library or in real time (chat-type system).

Whether communicating by email or in real-time, libraries should limit the personal information requested to only what is needed to provide the service. They must also state why the information is being collected, what authorizes the library to collect the information, and how to contact someone who can help them if they have questions regarding the collection (Act, s. 26). Also, individuals should be warned if the connection is not secure (e.g. encrypted).

Libraries using a real-time , method of communicating with individuals over the internet must consider the details of how the system works to ensure that the personal information collected is protected. A Privacy Impact Assessment (PIA) should be conducted to examine the privacy effects of an existing system or to ensure that any future system is in compliance with *FOIPPA*.

See "Policies & procedures: Privacy Impact Assessment (PIA)" for more information.

iii) On-line through an outside service provider

If individuals are simply referred to the website of an organization outside the library for help with reference questions, the library should clearly indicate this and recommend that the individual read the service's privacy policies.

When a library contracts with an outside organization to provide services on its behalf, the library is responsible for how personal information is treated by the organization because it is still under the library's "control" (Act, s. 3(1)).

The details of a reference system offered by an outside provider on behalf of the library must be examined to thoroughly consider the privacy implications. A Privacy Impact Assessment (PIA), should be conducted to examine the privacy effects of an existing system or to ensure that any future system is in compliance with *FOIPPA* before it is implemented.

See "On-line Services: Outside Databases", "On-line Services: On-line reference questions", "Outside Services Providers: Services provided on behalf of the library" and "Policies & Procedures: Privacy Impact Assessments" for more information.

c) Questions referred to other libraries or resources

Occasionally, a library has to consult with another library, or an outside organization to answer a question. Libraries should not forward the individual's personal information with the question. Most libraries seek out the information on behalf of the individual and then provide it directly to them. This is the best practice.

If it is not practicable to ask on the individual's behalf without disclosing her personal information, the library should provide the individual with the other organization's contact information so she can ask directly. If this is not possible or desirable, the library should follow the guidelines set out for Interlibrary Loans in Box 9.2 (in the next section).

7. Employee & Volunteer Personal Information

Employee and volunteer personal information is also protected under *FOIPPA*. Records containing personal information about employees and volunteers should be kept secure. Only other employees or volunteers who "need to know" should have access to the information.

Box 7.1

Examples of who may "need to know":

- *Employee & volunteer timesheets* → those responsible for supervising employees & volunteers or for payroll.
- *Criminal record check reports* → those responsible for screening employees and volunteers in this regard (e.g. Human Resources Director, Chief Librarian or Board members).

a) Surveillance

Surveillance, such as Close Circuit TV, any other audio/visual recording device, or keystroke monitoring, should be used only as a last resort. The B.C. Privacy Commissioner has set out guidelines for determining whether surveillance is necessary. A summary of these guidelines is provided under "Security: Surveillance Systems".

If the personal information collected through surveillance is used to make a decision that affects the individual, the library must keep the record (the surveillance tape) for at least one year, so the employee it belongs to can access it (Act., s. 31(b)). Otherwise, the record should be destroyed as soon as its purpose has been met.

b) Work contact information

Information needed to contact a library employee at work is *contact information* and is not considered *personal information* under *FOIPPA*. *Contact information* includes name, title, and work address/phone/fax/email (Act, Schedule 1). That means that this information is not regulated or protected by *FOIPPA*.

c) Pseudonyms

Library employees or volunteers may wish to use pseudonyms when dealing with the public in circumstances that may make them feel exposed to safety concerns. One example of this may be where they are communicating with individuals over the internet, especially in real-time (chat) where individuals using the service are anonymous.

8. Personal Information Access & Correction

Individuals have a right to request access to or a correction of their own personal information (Act, s. 4 & 29). Routine information access or correction, such as access to borrowing history or a change of address, may be facilitated by any employee or volunteer with authority. Non-routine requests for access or correction should go through the library's *FOI/Privacy Officer* (Act, s. 5).

a) Access to routine information

Where possible, individuals should be given routine access to their own personal information, such as their borrowing history (if applicable) and current address on record. Care is needed to ensure that it is actually the individual the personal information relates to that is gaining access.

Access by employees or volunteers to patron information should be on a need to know basis only (see "Security"). Those employees or volunteers who are authorized to help individuals access their own personal information should only do so when individuals are having difficulties accessing the information on their own.

b) Access to non-routine information

Patrons should be referred to the library's *FOI/Privacy Officer* to apply formally for access and corrections to non-routine information (e.g. for notes employees or volunteers may have recorded regarding them) (Act, s. 5). This is particularly important because there are instances where the library is required to withhold certain information. The *FOI/Privacy Officer* is the best person to make this determination.

c) Correction of personal information

Employees or volunteers with authority to do so may make routine corrections, such as change an address (Act, s. 77(b)). However, only the individual herself should be permitted to provide her change of address (unless it is for her child's card, debt collection purposes, or another purpose where *FOIPPA* allows collection indirectly - see Act, s. 27(1)). Non-routine corrections should be referred to the library's *FOI/Privacy Officer* (Act, s. 29).

d) Children

Children who are "capable" of doing so may exercise their own rights to access or correct their personal information (Reg., s. 3).

Libraries may also have policies allowing parents or guardians to access or correct their child's personal information where the child is under 12 years.

If a child under 12 objects to her parent accessing or correcting personal information about her, or if a child is over 12, the parent's request should be referred to the library's *FOI/Privacy Officer*. This can be a complex area and the *FOI/Privacy Officer* is in the best position to determine what is appropriate.

Box 8.1

Examples of when the *FOI/Privacy Officer* may give a parent access to a child's personal information:

1. Where
   a) the parent has custody of the child,
   b) the child is too young to be capable of exercising her own right to access the information, and
   c) the parent is attempting to exercise that right *on behalf of the child* (not in the parent's own interests) (Reg., s. 3).
2. Where there are "compelling circumstances affecting anyone's health or safety" (See Act, s. 22(4)(b) for more information).

e) Others (employees, volunteers, donors)

Employees, volunteers and donors also have the right to access and correct their personal information. Requests should be handled as outlined above.

9. Disclosure of Personal Information

Libraries must not disclose personal information unless they have the written consent of the individual the information belongs to or they are otherwise authorized to do so under *FOIPPA* (Act, s. 33). Requests for access to personal information belonging to anyone other than the person the information belongs to should be referred to the library's *FOI/Privacy Officer* (Act, s. 5).

a) Family & friends

Libraries should not disclose personal information of a patron to the patron's family or friends unless the library has written consent from the patron (Act, s. 33.1(1)(b)). Written consent must specify to whom the personal information may be disclosed and how the personal information may be used (Reg., s. 6).

b) Police

Requests for personal information by the police should be referred to the library's *FOI/Privacy Officer*. In addition to allowing personal information to be disclosed in order to comply with a subpoena, warrant or other order, personal information may be disclosed to the police to assist in a specific law enforcement investigation (Act, s. 33.2). The *FOI/Privacy Officer* will ensure

the police agency provides evidence of the appropriate authority for collecting the information.

c) Social workers and school counsellors

Requests for personal information by social workers or school counsellors should be referred to the library's *FOI/Privacy Officer* (Act, s. 5).

Box 9.1

Examples of when the *FOI/Privacy Officer* may disclose information:

- A B.C. or Canadian statute requires or allows the disclosure (Act, s. 33.1(1)(c)).
- The *FOI/Privacy Officer* determines there are compelling health and safety concerns. A notice must be sent to the person the information is about, unless doing so would harm someone's health or safety (Act, s. 33.1(1)(m)).
- So that the next of kin or a friend of someone who has been injured, become ill or died may be contacted (Act, s. 33.1(1)(n)).

d) Collection agencies

Requests for personal information by collection agencies should be referred to the library's *FOI/Privacy Officer*. If a collection agency calls the library for information about a patron, employee, or volunteer, the personal information should not be disclosed unless the agency can provide evidence that they have a valid subpoena, warrant or other court order compelling the library to disclose the personal information (Act, s. 33.2(b)).

Where a collection agency is contracted by the library, to collect a debt owed to the library, personal information may be disclosed to collection agency without consent from the individual the information is about (Act, s. 33.1(1)(i)). However, only the personal information reasonably needed by the collection agency should be provided. Additionally, the personal information must not be disclosed outside Canada unless it is reasonable to believe that the person who owes the debt lives or has assets in that country (Act, s. 33.1(1)(i)).

See "Collection agencies" under "Registration", "Outside service providers", and "Circulation: Unreturned materials" for more information.

e) Other libraries

There may be a number of reasons why a library may wish to disclose personal information to (or collect from) another library, such as for interlibrary loans, in an effort to collect a debt owed for unreturned items, or where the library is investigating a breach of its rules. All personal information sharing practices with other libraries should be approved by the library's *FOI/Privacy Officer*.

Cont'd...

Box 9.2

Examples:

- *Interlibrary loans:* Libraries should avoid disclosing personal information to other libraries within the interlibrary loan process. However, where this is not possible, the following guidelines should be followed:
    a. *Within* B.C.: A library may disclose personal information to a library within B.C. for the purpose of an interlibrary loan if it was obtained for that purpose. When the personal information is collected, the patron must be told the purpose for collecting the information, the legal authority for collecting it and the contact information for the library's *FOI/Privacy Officer*.
    b. *Outside* B.C.: In addition to what is set out in (a), the form should also contain a notice that the patron's personal information is being disclosed to a library outside of B.C., where the privacy protection laws may not protect against access or disclosures outside of Canada.
    c. *Outside Canada:* Patrons must provide written consent for their personal information to be disclosed outside Canada (Act, s. 33.1(1)(b)). The consent form must state to whom the information may be disclosed and how it may be used (Reg., s. 6) (see "Disclosure, storage or access outside Canada for more information").
- *Debt collection*: Libraries may ask other libraries for personal information about a patron for the purpose of collecting a debt owed by that individual (Act, s. 33.1(1)(i)(i)). For example, a library may ask if a certain patron is registered in another library and request the address the patron provided.
- *Objectionable behaviour:* Libraries may disclose personal information without consent for the purpose of an investigation the library is conducting that may lead to imposing a penalty or sanction on a specific individual (e.g. asking another library if it has a patron's address so that a notice of fine may be sent to her) (Act, s. 33.2(a)) or where there are compelling health or safety concerns (Act, s. 33.1(m)).
- *Black lists:* Libraries should not share "black lists" or otherwise share information about patrons unless disclosure is allowed under section 33.1 or 33.2 of *FOIPPA* (e.g. in order to collect a debt or as part of an investigation that may lead to imposing a penalty or sanction – see above).

See "Collection agencies" (above), "Circulation: Unreturned Materials", "Miscellaneous: Objectionable behaviour of patrons" for more information.

10. Records Retention & Disposal

a) In general

Personal information should only be kept as long as is reasonably necessary (although *FOIPPA* does not provide limits on how long public bodies may keep personal information). However, where personal information is used to make a decision that affects an individual to whom it belongs, the library must keep the information for a minimum of one year, so that the individual can access the information (Act, s. 31).

When personal information is destroyed, a method secure should be used that is appropriate and effective for the media (see Box 10.1 (below) for some tips).

Box 10.1

TIPS on destroying personal information:

- *Paper:* Should be shredded (ideally using a cross-shredder), burned or pulped. Never throw paper with personal information into a recycle bin unless it is in a secure location and stays secure until it is shredded.
- *Computer data:* Data is not destroyed simply by "deleting" the file. Deleting merely removes the file name from the directory and allows the data to be overwritten eventually. Erasable media (such as disks, hard drives, CDs, DVDs) should be purposefully overwritten, "wiped", or "sanitized", using software designed specifically for the purpose. The safest method of destroying data is to physically destroy the media (just cutting CDs in half isn't enough). Non-erasable media should be physically destroyed.

b) Back-ups

When personal information is destroyed, it is important to also remember to consider whether there is a back-up of the information as well. If so, the personal information there must also be destroyed (see Box 10.1 above).

c) Borrowing history

Libraries should not keep a history of what materials patrons have borrowed, except where they have the individual's consent. Reference to the item being borrowed should be removed from the patron record, as soon as possible, when the item is returned.

See "Circulation: History of what a patron borrowed" for more information.

d) Book/resource history

A patron's personal information should only be associated with a borrowed resource until the record is no longer needed.

See "Circulation: History of who borrowed an item" for more information.

11. Outside Service Providers

a) Services provided on behalf of the library

When an outside organization is used to provide library services on behalf of a library, it is as though the library was providing the service itself. In other words, the library is responsible for how the service provider deals with

personal information in the course of providing services for the library (Act, s. 3(1)). It is important to know exactly how the personal information will be treated in every aspect of the service.

A Privacy Protection Schedule (PPS) should form part of any contract involving personal information. A pre-written PPS is available on-line at http://www.mser.gov.bc.ca/privacyaccess/PPS/default.htm.

Box 11.1

Examples of 2 Extremes:

- *Mail house*: Where a library uses a mail house for mass mailings, it should clearly set out that the personal information is in its control while at the mail house and specify how the mail house must comply with *FOIPPA*. A Privacy Protection Schedule (PPS) should form part of the contract for services (see above).
- *Software service providers*: This is a far more complex area. The flow of personal information can be complex and pose problems for securing the information. Also, the organizations often store patron personal information on their own servers and in providing technical services, their employees may access the personal information. If the company is not Canadian, the situation is even more complex because it is illegal to store or access personal information outside Canada, except in certain circumstances (Act, s. 30.1). When considering having an outside organization provide this type of service, libraries should conduct a Privacy Impact Assessment (PIA).

See "Policies & Procedures: Privacy Impact Assessment (PIA)" for more information. Also see the "Guidelines for Data Service Contracts", written by the Office of the Information & Privacy Commissioner (May 8, 2003, Ref 01-02), available on the Commissioner's website at http://oipc.bc.ca/Guidelines-Data_Services.pdf.

b) Referrals to services or organizations outside the library

i) On-line services

Libraries often refer patrons to services that are hosted on other organization's websites (e.g. live tutoring sites, outside database subscription services, and library materials-due alert services). It is important to let individuals know that they are going to another organization's website and to recommend that they read that organization's privacy policies.

See also "On-line Services: Outside databases" and "Reference Questions: Questions referred to other libraries or resources".

ii) Collection agencies

Libraries may want to use a collection agency to collect a debt. Personal information may be disclosed to a collection agency without consent from the individual to whom it belongs for this purpose (Act, s. 33.1(1)(i)). Only personal information reasonably needed by the collection agency should be disclosed. Also, the personal information must not be disclosed outside Canada unless it is reasonable to believe that the person who owes the debt lives or has assets in that country (Act, s. 33.1(1)(i)).

Contracts with collection agencies should have a Privacy Protection Schedule (PPS) attached to form part of the contract. The PPS specifies how the collection agency must treat the personal information. The Information Policy & Privacy Branch offers a PPS available on-line at http://www.mser.gov.bc.ca/privacyaccess/PPS/default.htm.

For more information, see "Collection agencies" (above), as well as under "Registration" and "Disclosure of personal information".

c) Janitorial or other services

Whether janitorial or other services are provided by employees or outside service providers, it is unlikely that there is any reason why they should need access to personal information in the custody of the library. Security and training measures should be taken to ensure that persons without authorization do not access personal information.

12. Security

Libraries must take reasonable steps to ensure that personal information in their custody or under their control is secure against unauthorized collection, use, access, disclosure, or disposal (Act, s. 30).

a) Authorized employees and volunteers

Only employees or volunteers who need access to personal information in the course of their work should be authorized to access personal information.

b) Confidentiality agreements

Libraries should have confidentiality agreements with employees and volunteers who are authorized to access personal information. The confidentiality agreements should stipulate that the employee/volunteer will comply with the requirements of *FOIPPA* and the library's privacy policies when dealing in any way with personal information and stipulate what steps may be taken to enforce the policies.

c) Training

It is important that employees and volunteers who are authorized to access personal information are properly trained in the requirements of *FOIPPA* and the library's privacy policies. Each employee and volunteer should know the

contact information for the *FOI/Privacy Officer* so that this information can be provided to whoever requests it.

d) Technology

Appropriate technological safeguards should be taken to protect personal information. These will depend on the particular system used by each library.

Box 12.1

Examples of technological safeguards:

- Where personal information is communicated electronically and could be intercepted by a third party, the communication should be secure (e.g. encrypted). If this is not feasible, then notice should be given that the communication is not protected and may be intercepted by a third party (see Appendix II: Sample Privacy Clauses).
- Employees and volunteers should be assigned user access profiles (IDs & passwords) so that databases containing personal information are only accessible by those authorized employees or volunteers.
- Controls should be in place to prevent those who do not have specific authority to add, change or delete personal information from doing so.
- All personal information exchanges and storage should be protected (e.g. firewalls, encryption).
- The system security should include an audit process that can track use of the system and identify inappropriate access to the system.
- Access profiles and passwords of former employees and volunteers should be deleted immediately upon leaving.

e) Physical security

Personal information recorded on any media (including paper, CPUs, servers, and other electronic media) should be physically protected. Areas where personal information is stored should only be accessed by authorized employees and volunteers. This may require organizing space in order that personal information is stored separately in an area non-authorized personnel do not need to enter.

Box 12.2

More examples of securing personal information:

- *Sensitive personal information*, such as employee criminal record check reports or Home Service patron's medical information, should be stored separately in a secure area that is only accessible by employees authorized to access that particular information.
- *Screens of terminals* that are used to access or change personal information should not be visible to unauthorized persons, including other employees, volunteers or patrons. A privacy filter screen may help protect personal information on the screen.
- *When deleting or disposing of personal information*, a method should be used that is appropriate to the type of media (see "Records retention & disposal" for more information).
- *Lock file cabinets and doors to rooms* where personal information is stored during times when the area is not under the supervision of authorized employees or volunteers.
- *An appropriate security system* should be used to protect personal information during times when the area is not under the supervision of authorized employees or volunteers. For example, personal information should be inaccessible to janitors and night staff who are not authorized to access personal information.

f) Surveillance

Close Circuit TV (CCTV) or other audio, visual or electronic surveillance should only be used as a last resort. Libraries should be prepared to show that other means are *substantially* less effective and that the benefits of surveillance *substantially* outweigh the lessening of privacy caused by the surveillance used.

Box 12.3

Factors to consider:

- The surveillance system must be justified using verifiable information, such as incident reports.
- A Privacy Impact Assessment (PIA) should be conducted before implementing a surveillance system.
- Stakeholders should be consulted when reviewing whether or not to implement a surveillance system.
- The surveillance system should be designed so that it achieves its goals with the least privacy invasion possible.
- The surveillance equipment should only monitor identified public areas.
- Notices should be prominently displayed around the area being monitored, informing individuals that the area is under surveillance so that they are aware of the surveillance before entering the area.
- Only authorized employees should have access to the equipment and storage devices.
- Audits should be conducted at irregular intervals to review the use and security of the equipment.
- Comprehensive privacy policies should be created for operating the system, as well as use and retention of the recorded information.

For more information, see the "Public Surveillance System Guidelines", written by the Office of the Information & Privacy Commissioner (January 26, 2001, Ref 00-01), available at http://oipc.bc.ca/advice/VID-SURV.pdf.

13. Miscellaneous

a) Disclosure, storage or access outside Canada

Libraries must not disclose or store personal information outside Canada, or allow it to be accessed from outside Canada, with certain exceptions (Act, s. 30.1). One exception is where the individual the personal information belongs to has consented in writing, after being told where the information will be stored or from where it will be accessed, to whom it may be disclosed, and how it may be used (Reg., s. 6).

Cont'd...

If consent is taken electronically, there must be a method of authenticating the identity of the person so the library may be assured it is the person herself who is consenting.

Box 13.1

What about existing contracts involving storage/access outside Canada?

- The changes made to *FOIPPA* with respect to disclosure, storage and access of personal information outside Canada became effective on October 21, 2004.
- The changes do not apply to contracts entered into by a library before the effective date (October 21, 2004) until the end of the term of the contract (subject to the information below).
- However, once the term originally set in a contract entered into before October 21, 2004 expires, the new provisions apply (i.e. if an amendment was made after October 21, 2004 that extended the term of the contract, the changes to *FOIPPA* requiring storage/access in Canada would apply as of the original end date set in the contract).
- Additionally, libraries are legally required to make all reasonable efforts to make contracts entered into before October 21, 2004 compliant as soon as reasonably possible.

See the *Freedom of Information and Protection of Privacy Amendment Act*, 2004 for more information. Information on how to access the Act is provided in Appendix I.

b) Library system changes

Libraries should conduct a Privacy Impact Assessment (PIA) whenever a new system is being developed or purchased that will collect, use, retain or disclose personal information (Act, s. 69(5) & (7)). This will allow the library to deal with any potential privacy concerns prior to implementing the new system. The library's Personal Information Directory (PID) should be updated to reflect the changes as well (Act, s. 69(2) & (7)).

See "Policies & Procedures: Privacy Impact Assessment (PIA)" and "Policies & Procedures: Personal Information Directory (PID)" for more information.

c) Objectionable behaviour of patrons

Libraries may record personal information about patrons in order to enforce established rules, impose fines or suspend library privileges for breaches of library rules, or to exclude someone who has behaved in a disruptive manner or who has damaged library property (Act, s. 27(1)(c)(iv)).

Personal information collected for this purpose must not be disclosed to other libraries, unless it is for the purpose of an investigation the library is conducting that may lead to the library imposing a penalty or sanction on a specific individual (Act, s. 33.2(a)).

d) Room rentals

Personal information about individuals who book or rent space at the library should not be disclosed to other individuals (Act, s. 33).

If a list is used to record the personal information (such as name or address) of individuals who book rooms in the library, the list should be completed and viewed only by authorized employees and volunteers.

The lists should only be kept for as long as is reasonably necessary, such as to record statistical information. Once the lists are no longer necessary, they should be disposed of in a way that is appropriate for the media used (such as shredding paper and "wiping" or "sanitizing" computer disks).

See "Records retention & disposal" for more information.

e) Donor personal information

Donor personal information must be protected in the same way that any other personal information is protected.

Box 13.2

TIPS for taking care of donors' personal information:

- Donors should be informed about the purpose(s) for collecting their personal information, how it will be used, and how it will be disclosed (if at all) when collecting their personal information.
- Donor personal information should be kept secure and only accessible to employees or volunteers who need access to it in order to fulfill their work responsibilities.
- Libraries should get the consent of a donor if they wish to publicly acknowledge the donor's membership or contributions.

f) Research

Where a library wishes to disclose information for the purposes of research, the best practice is to ensure that the information is stripped of any personal information (which includes any type of information that could reasonably be used to identify the individual).

Libraries may only disclose personal information for research purposes where *FOIPPA*'s specific requirements for this purpose are met (Act, s. 35).

Cont'd

Box 13.3

FOIPPA's requirements for disclosing personal information for research purposes:

1. The research cannot be reasonably accomplished without personal information or the Commissioner has approved the research;
2. the information is disclosed on the condition that it will not be used to contact the individuals to ask them to participate in the research;
3. any linking of records is not harmful to the individuals and the linkage benefits are clearly in the public interest;
4. the head of the library (person ultimately responsible for the library's compliance with *FOIPPA*) has approved the following conditions:
   a) security and confidentiality;
   b) removal and destruction of individual identifiers as soon as possible;
   c) prohibition of any further use of disclosure of the personal information without express authorization from the library; and
5. the person to whom the personal information was disclosed has signed an agreement to comply with the approved conditions, *FOIPPA*, and the library's privacy policies and procedures (Act, s. 35).

14. Policies & Procedures

Libraries should have written policies and procedures outlining their personal information practices. These policies and procedures must be available to the public (Act, s. 70).

a) Privacy policies

The library's privacy policies should cover all areas of the library's programs and functions that involve personal information in any way. All the policies may be in one document, or they can be separated by context (such as general and website policies).

Box 14.1

Privacy policies should include the following information:

1. Contact information for the library's *FOI/Privacy Officer*.
2. The library's authority for collecting personal information.
3. The purposes for which the library collects personal information.
4. How personal information will be used.
5. How long personal information will be retained.
6. A statement regarding accuracy and completeness of personal information.
7. How personal information is protected.
8. How individuals may access information about policies and procedures.
9. How individuals may request access to or correction of their personal information.
10. To whom individuals may make inquiries regarding how their personal information is treated by the library.

See Appendices III & IV for sample privacy policies.

i) General

Libraries should have privacy policies that cover the personal information practices of the library in general, such as those pertaining to registration, circulation, Home Service, computer use, and surveillance (if relevant).

See "Appendix IV: Sample general privacy policy".

ii) Website

Libraries should include information about how they collect, use or disclose personal information via their website as part of their general privacy policies and/or provide separate privacy policies for the website. The website policies should be available from the library's main web page.

See "Appendix III: Sample website privacy policy".

b) Procedures – Instructions to employees & volunteers

Employees and volunteers should be instructed on proper procedures for handling personal information in the various areas of the library that are relevant to the work of the employee or volunteer. Written instructions should be provided. These instructions must be made available to the public upon request (Act, s. 70) .

i) Training

All employees and volunteers should receive training regarding proper treatment of personal information and regarding the library's privacy policies . Employees and volunteers who are authorized to access personal information as part of their work functions should have detailed and specific training relevant to the scope of their authorization.

ii) Communication of policies to patrons

Employees and volunteers must let individuals know how they can access information about the library's privacy policies and procedures when requested or when otherwise appropriate (Act, s. 70).

iii) FOI/Privacy Officer

The library must have a *FOI/Privacy Officer*, who is the designated employee responsible for the library's compliance with *FOIPPA* (Act, s. 77(a)). All requests for access to personal information (unless routine, such as change of address) and privacy complaints, should be referred to the *FOI/Privacy Officer*.

c) Personal Information Directory (PID)

Libraries should prepare and maintain a Personal Information Directory (PID) that provides the public with information about what kind of personal information the library has and for what the personal information is used (Act, s. 69(2) and (7)).

The PID should include a summary of the following information:

1. the personal information banks that the library has in its custody or under its control;

2. any information sharing agreements the library has entered into; and

3. any Privacy Impact Assessments (PIAs) the library has conducted.

Box 14.2

What do those terms mean?

- *Personal Information Directory (PID)* – means a collection of personal information that is organized or retrievable by the name of an individual or any other identifying information, such as a number, *barcode* or other identifying symbol particular to that individual.
- *Privacy Impact Assessment (PIA)* – means an assessment that is done in order to determine whether or not a new system, law, project, or program meets the personal information protection requirements of *FOIPPA* (see below).
- *Custody* – means the personal information is physically in the public body's or organization's custody.
- *Control* – means the personal information is under the control of the public body, even if it is actually in the custody of another public body or organization.

d) Privacy Impact Assessment (PIA)

Libraries should conduct a Privacy Impact Assessment (PIA) each time a new system, project or program is being considered (s. 69(5) & (7)). A PIA considers a comprehensive list of factors that are important in determining whether or not the new system, project or program will protect personal information in a way that is compliant with *FOIPPA*.

See the Information Policy & Privacy Branch's website for a PIA template. Their contact information is available under "Additional Resources" under "Appendix I: Helpful contact information".

Appendix I – Additional Resources

a) Legislation

- **B.C.'s *Freedom of Information & Protection of Privacy Act (FOIPPA)***, on-line at http://oipc.bc.ca/legislation/FOI-ACT%20(webversion)15Dec05.pdf.
    - **Regulations**, on-line at http://oipc.bc.ca/legislation/Reg%20323_93%20(2004).pdf.
    - ***Freedom of Information and Protection of Privacy Amendment Act, 2004***, on-line at http://www.legis.gov.bc.ca/37th5th/3rd_read/gov73-3.htm.
- **B.C.'s *Personal Information Protection Act (PIPA)***, on-line at http://oipc.bc.ca/legislation/PIPA2003%20(2004).pdf.
    - **Regulations**, on-line at http://www.qp.gov.bc.ca/statreg/reg/P/473_2003.htm.
- **Canada's *Privacy Act***, on-line at http://lois.justice.gc.ca/en/P-21/index.html.
    - **Regulations**, on-line at http://lois.justice.gc.ca/en/P-21/SOR-83-508/index.html.
- **Canada's *Personal Information Protection and Electronic Documents Act (PIPEDA)***, on-line at http://lois.justice.gc.ca/en/P-8.6/.
    - **Regulations Re: Publicly Available Information,** on-line at http://lois.justice.gc.ca/en/P-8.6/SOR-2001-7/text.html.

b) Helpful contact information

- **Information Policy & Privacy Branch**
  Ministry of Labour & Citizens' Services
  Tel: 250.356.1851 (Victoria)
  Toll free: Call Enquiry B.C. at 604.660.2421 (Vancouver) or 1.800.663.7367 (elsewhere in B.C.) and request a transfer to 250. 356-1851.
  Email: CPIAADMIN@gov.bc.ca
  Website: http://www.mser.gov.bc.ca/privacyaccess/

Cont'd...

- **Office of the Information and Privacy Commissioner (OIPC)**
  Tel: 250.387.5629 (Victoria)
  Toll free: Call Enquiry B.C. at 604.660.2421 (Vancouver) or 1.800.663.7367 (elsewhere in B.C.) and request a transfer to 250.387.5629.
  Email: info@oipc.bc.ca
  Website: http://oipc.bc.ca

- **Office of the Privacy Commissioner of Canada**
  Tel: 613.995-8210 (Ottawa)
  Toll free: 1.800.282.1376
  Email (for requesting publications): publications@privcom.gc.ca
  Website: www.privcom.gc.ca/

c) Helpful documents

- **"Faxing and Emailing Personal Information" Guidelines** (B.C. Office of the Information & Privacy Commissioner), on-line at http://oipc.bc.ca/pdfs/public/fax-emailguidelines(Feb2005).pdf.

- **"Guidelines for Using RFID Tags in Ontario Public Libraries"** (Office of the Information and Privacy Commissioner of Ontario), on-line at http://www.ipc.on.ca/docs/rfidgdlines.pdf.

- ***Libraries Without Walls: The World Within Your Reacn*** (Public Library Services Branch, B.C. Ministry of Education, 2004), online at http://www.bced.gov.bc.ca/pls/library_strategic_plan.pdf.

- **Privacy Impact Assessment template** (Information Policy and Privacy Branch, B.C. Ministry of Labour and Citizens' Services), on-line at http://www.mser.gov.bc.ca/privacyaccess/PIA/PiaTemplateRevised05.doc.

- **Privacy Protection Schedule (PPS) for public bodies** (Information Policy and Privacy Branch, B.C. Ministry of Labour and Citizens' Services), on-line at http://www.mser.gov.bc.ca/privacyaccess/PPS/default.htm

- **"Public Surveillance System Guidelines"** (B.C. Office of the Information & Privacy Commissioner, January 26, 2001, Ref 00-01), on-line at http://oipc.bc.ca/advice/VID-SURV.pdf.

- **Supplement to the Core Policy and Procedures Manual**, Chapter 12, Information and Technology Management Manual, 12.3.2 I h "Destruction of Records" (B.C. Ministry of Labour and Citizens' Services), on-line at http://www.cio.gov.bc.ca/prgs/CPM12.pdf.

Appendix II – Sample Privacy Clauses

The following clauses may be helpful for libraries in writing their own. Please keep in mind that these clauses only address personal information protection issues. They do not speak to other concerns, such as responsibility for borrowed resources or children's internet use.

a) Authority to collect personal information

ABC Library's legal authority to collect personal information flows from the *Library Act* and section 26 of the *Freedom of Information and Protection of Privacy Act*. Other acts may also authorize specific information collected, such as the *Income Tax Act*.

b) Registration form

The information on this form is collected under the authority of the *Library Act* and section 26 of the *Freedom of Information and Protection of Privacy Act*. The information will be used only as allowed by law, such as to assess your eligibility for borrowing privileges, which may involve enquiring into your debt status with other libraries; to contact you about reserve materials; or to collect overdue materials. For questions about the collection or use of this information, please contact the library's FOI/Privacy Officer, [Name], [Address], [City], B.C., [Postal Code], Phone: [Phone #].

c) Un-secure communication from website

This is not a secure site. Individuals using this form to submit information to the library should be aware that the communication is not encrypted nor secured in any way. It is therefore possible for the information to be intercepted by another person. If you would prefer to phone or fax your personal information, please call (xxx) xxx-xxxx.

Appendix III – Sample Website Privacy Policy

The purpose of this sample policy

This sample website privacy policy was written to help libraries develop their own website privacy policies. Care should be taken to ensure that your policy accurately reflects the personal information practices of your own library.

Each library is responsible for its own compliance with *FOIPPA* and should use its own best judgment in discharging its duties under *FOIPPA*.

ABC Library - Website Privacy Policy

[Last reviewed: Date]

1. Introduction

ABC Library is committed to protecting your privacy. Any personal information collected, used or disclosed by ABC Library is in accordance with the *Freedom of Information and Protection of Privacy Act* (*FOIPPA*).

2. What is personal information?

Personal information is defined by *FOIPPA* as information about an identifiable person. Some examples of personal information are name, age, home address, phone number, email address, IP address (a computer's address), identification numbers, reading choices and age. *FOIPPA*'s definition of personal information does not include work contact information, which is information that would allow a person to be contacted at a place of business, such as the person's name, title, business address, business phone number, and business email address.

3. Information automatically collected when visiting our site

Some information is automatically collected by our server when you browse our website, including

- the domain name and IP address of the computer you are using;
- your browser and operating system;
- the screen resolution;

- the date and time you accessed the site;
- what pages you visited; and
- what website you visited from, if applicable.

We collect this information to help make our site more useful by assessing our web services and system performance, as well as learning how many people are visiting the site and how they are using it. No attempt is made to use this information to identify visitors, unless it is necessary for an investigation or it is required by law.

4. Personal information collected via email and web forms

Your personal information is collected by ABC Library when you fill-in a library web form or send an email, such as when you apply for a library card online, ask a reference question, or offer book suggestions.

Personal information you send to us by email or when using our web forms will only be used by authorized staff for the purpose for which it was collected or for a consistent purpose, unless you consent otherwise, or it is authorized or required by law.

Information you send to ABC Library using our web forms is encrypted so that it is protected from a third party accessing it in transit. However, email messages sent over the internet are not secure and may be read by a third party who intercepts the communication. If you are concerned about sending your personal information over email, we suggest you either phone or fax us instead.

5. Cookies

Cookies are small files that are saved on your computer and used to store information that is communicated back to the website being accessed.

ABC Library uses cookies to help you move around our website. These cookies do not store personal information. It is possible to change the settings on your browser so that cookies will be denied or so that you will be warned before a cookie is saved on your computer.

6. Security

ABC Library uses reasonable security measures to protect against risks such as unauthorized access, collection, use, disclosure or disposal.

These security measures protect personal information once it reaches our server. ABC Library's security cannot protect information while it is in transit over the internet, unless the information is collected by one of our secure online web forms. Information sent to ABC Library in email messages is not secure.

7. Links to other sites

ABC Library strives to provide a wealth of resources from our website, including links to sites outside of the library, such as encyclopedias, reference databases, tutoring help, and private organizations.

ABC Library has no control over the management of these web sites and we are not responsible for their privacy policies. You are encouraged to review those policies before using the service or providing any personal information.

8. How long is personal information kept?

How long ABC Library keeps your personal information depends on the nature of the service for which the information was collected.

If ABC Library uses your personal information to make a decision that affects you, we must keep that information for at least one year so that you have an opportunity to access it. Otherwise, we keep it for the length of time necessary to fulfill the purposes for which it was collected. Personal information is securely destroyed when it is no longer needed.

9. Disclosure of personal information

ABC Library does not sell or rent personal information. Personal information is disclosed only in accordance with *FOIPPA* or as required by law.

10. Accuracy of personal information

ABC Library will endeavour to ensure the personal information is as accurate, complete and up-to-date as necessary.

11. How can I access or correct my personal information?

To access your personal information held by ABC Library, submit a written request to ABC Library's FOI/Privacy Officer (see contact information below). Your request should provide enough detail to enable

a library employee to find the personal information (e.g. "personal information I submitted when I applied for a library card online").

You may request that the personal information about you by ABC Library be corrected if you believe it is incorrect. You may do so by submitting your request in writing to the FOI/Privacy Officer (see contact information below).

12. Changes to this Privacy Policy

ABC Library's practices and policies are reviewed from time to time. Any changes to these policies will be posted on this site.

13. Who can I contact about ABC Library's privacy policies?

If you have any questions or concerns about this policy or how ABC Library treats your personal information, you may contact our FOI/Privacy Officer.

Name
Title
ABC Library
Address
City, B.C. Postal Code
Phone
Email

If you are not satisfied with how your complaint was handled by ABC Library, you have the right to complain to the Office of the Information and Privacy Commissioner [http://oipc.bc.ca].

14. Links

- The *Freedom of Information and Protection of Privacy Act* (*FOIPPA*) and its Regulations can be accessed from the Office of the Information and Privacy Commissioner's website [http://oipc.bc.ca/legislation.htm].
- The website of the Information Policy and Privacy Branch of the Ministry of Labour and Citizens' Services contains a wealth of information about *FOIPPA* and the guidelines and policies that govern the legislation [http://www.mser.gov.bc.ca/privacyaccess].
- ABC Library's General Privacy Policy
- Other library polices

Appendix IV – Sample General Privacy Policy

The purpose of this sample policy

This sample website privacy policy was written to help libraries develop their own general privacy policies. Care should be taken to ensure that your policy accurately reflects the personal information practices of your own library.

Each library is responsible for its own compliance with *FOIPPA* and should use its own best judgment in discharging its duties under *FOIPPA*.

ABC Library – General Privacy Policy

[Last reviewed: Date]

1. Introduction

ABC Library is committed to protecting your privacy. Any personal information collected, used or disclosed by ABC Library is in accordance with the *Freedom of Information and Protection of Privacy Act* (*FOIPPA*).

2. What is personal information?

Personal information is defined by *FOIPPA* as information about an identifiable person. Some examples of personal information are name, age, home address, phone number, email address, IP address (a computer's address), identification numbers, reading choices and age. *FOIPPA*'s definition of personal information does not include work contact information, which is information that would allow a person to be contacted at a place of business, such as the person's name, title, business address, business phone number, and business email address.

3. Collection of personal information

When collecting personal information from you, ABC Library will advise you of the purpose for collecting it and the legal authority for doing so. We will also provide you with contact information of the library's FOI/Privacy Officer, who can answer your questions regarding the collection.

The following are some example of purposes for which ABC Library may collect your personal information:

- issuing library cards
- identifying materials currently on loan
- placing and tracking inter-library loans
- identifying and recording overdue materials
- placing and tracking materials on hold
- providing answers to reference questions
- faxing materials
- providing information about library programs and services
- providing Home Service for patrons with special needs
- recording book suggestions
- recording comments or suggestions
- general library operations
- library fundraising

Patrons who do not wish to be contacted about library services and programs or for fundraising purposes may choose to opt-out.

4. How is personal information used?

ABC Library will only use your personal information for the purposes for which it was originally collected or in a manner that is consistent with those purposes. The library will only use your personal information for different purpose if you explicitly consent to the new purpose or the use is authorized under *FOIPPA* or is otherwise required by law.

5. When is personal information disclosed?

ABC Library does not sell or rent personal information. Personal information is disclosed only in accordance with *FOIPPA* or as otherwise required by law.

Where other organizations require personal information in order to provide services on behalf of the library, ABC Library ensures that these organizations treat the personal information in compliance with *FOIPPA* and the library's privacy policies.

Examples of where personal information may be disclosed include:

- when a patron explicitly consents to the disclosure;
- to a collection agency for the purpose of collecting a debt;
- for law enforcement purposes, such as where required by a subpoena, warrant or other order;
- where there are compelling health and safety concerns; or
- to contact a person's next of kin if that person is injured, becomes ill or dies while visiting the library.

6. How is personal information kept secure?

ABC Library uses reasonable security measures to protect against risks such as unauthorized access, collection, use, disclosure or disposal.

Security measures include physical, technological and operational safeguards that are appropriate to the nature and format of the personal information.

7. How long is personal information kept?

How long ABC Library keeps your personal information depends on the purpose for which the information was collected.

If ABC Library uses your personal information to make a decision that affects you, we must keep that information for at least one year so that you have an opportunity to access it. Otherwise, the library will keep personal information only for the length of time necessary to fulfill the purposes for which it was collected. Personal information is securely destroyed when it is no longer needed.

8. Accuracy of personal information

ABC Library will endeavour to ensure the personal information is as accurate, complete and up-to-date as necessary.

9. How can I access or correct my personal information?

You have a right to request access to personal information held by ABC Library. To do so, you may submit a written request to ABC Library's FOI/Privacy Officer (see contact information below). Your request should provide enough detail to enable a library employee to find the personal information (e.g. personal information I provided when I applied for a library card).

You also have a right to request that your personal information held by ABC Library be corrected if you believe it is incorrect. You may do so by submitting your request in writing to the FOI/Privacy Officer (see contact information below).

10. Children's personal information

Children have the same rights as adults with respect to their personal information under *FOIPPA*. Where a child is "incapable" of exercising her right to access, correct or consent to the disclosure of his/her personal information, the child's parent or guardian may do so on her behalf.

ABC Library assumes that children 12 years are generally capable of exercising their own rights for policy purposes. However, the library may treat a request on an individual basis where a child or parent/guardian does not believe the guideline age is appropriate in their circumstances.

11. Changes to this Privacy Policy

ABC Library's practices and policies are reviewed from time to time. This policy will be updated to reflect the changes.

12. Who can I contact about ABC Library's privacy policies?

If you have any questions or concerns about this policy or how ABC Library treats your personal information, you may contact our FOI/Privacy Officer.

Name
Title
ABC Library
Address
City, B.C. Postal Code
Phone
Email

If you are not satisfied with how your complaint was handled by ABC Library, you have the right to complain to the Information and Privacy Commissioner:

Cont'd...

Office of the Information and Privacy Commissioner for British Columbia
PO Box 9038, Stn. Prov. Govt.
Victoria, B.C. V8W 9A4
Tel: 250.387.5629 (Victoria)
Toll free: Call Enquiry B.C. at 604.660.2421 (Vancouver) or 1.800.663.7367 (elsewhere in B.C.) and request a transfer to 250.387.5629.
Email: info@oipc.bc.ca
Website: http://oipc.bc.ca

Index

A

access to information, 2
access to personal information, 25
  in sample policy, 44, 48
accuracy of personal information, 36
  in sample policy, 44, 48
authenticating identity, 34
authority to collect personal information
  sample privacy clause, 41
automatic overdue notices, 14

B

back-ups, 21, 29
barcodes, 10
books on hold, 13

C

chat reference questions, 23
children, 7
  12 years and over, 8, 12, 25
    in sample policy, 49
  access to personal information, 25
  collecting personal information, 8
  correction of personal information, 25
  parent or guardian access, 25
  parent or guardian authorization, 8
  unreturned materials, 15
children's personal information
  in sample policy, 49
circulation, 10
collecting personal information, 4
  about a family member, 6
  children's, 8
  for computer use, 19
  for debt collection, 5
  for marketing or fundraising, 9
  for planning programs/services, 4
  for statistical purposes, 4
  home service, 8, 14
  ID numbers and references, 6
  in sample policy, 43, 46
  in smaller communities, 4
  limits, 4
  non-residents, 9
  notice for computer users, 18
  on-line reference questions, 17
  outside databases, 18
  patron ID, 5
  personal references, 6
  reference questions asked in person, 21
  surveillance, 24, 33
  to learn more about patrons, 4
  using surveillance, 21
  via email, 22
  via outside service provider, 23
  via website, 22
  what patrons need to know, 6
  when borrowing reference materials, 22
collection agencies
  contracts with, 31
  debt owed to library, 27
  disclosure of personal information, 15, 30
  information about patron, employee, or volunteer, 29
  request for personal information, 27
computer screens, 10
confidentiality agreements, 31
contact information, 24
  employees and volunteers, 24
  in sample policy, 42, 46
contracts
  personal information stored in/accessed from outside Canada, 34
cookies
  in sample policy, 43
correction of personal information, 25
  in sample policy, 44, 48

D

debt collection, 5, 6, 28
decision that affects the individual, 28
definitions, 3
  contact information, 3
  control, 38
  custody, 38
  FOI/Privacy Officer, 3
  personal information, 3
  Personal Information Directory (PID), 38
  Privacy Impact Assessment (PIA), 38
  record, 3
destroying personal information, 29
disclosure of children's personal information
  in sample policy, 49
disclosure of personal information, 26
  about employee or volunteer, 27
  black lists, 28
  books on hold, 13
  children, 8
  children's unreturned materials, 15
  donor personal information, 35
  examples of when may be allowed, 27
  for marketing or fundraising, 9
  for research, 35
  in sample policy, 44, 47
  outside BC, 28
  outside Canada, 27, 30, 33
  paper book cards, 14
  room rentals, 35

to a collection agency, 15, 27, 30
to collect unreturned materials, 14
to family and friends, 11, 26
examples, 11
to other libraries, 27
to other library for debt collection, 16
to police, 26
to school counsellors, 27
to social workers, 27
where objectionable behaviour, 34
disclosure, storage or access outside Canada, 33
donor personal information, 35

E

email address, 22
email to library
in sample policy, 43
emailing personal information, 16
employee and volunteer access, 10
employee and volunteer personal information, 24
employees, volunteers and donors
access to personal information, 26
encryption
in sample policy, 43

F

family and friends
disclosure of personal information, 26
family member
collecting personal information about, 6
faxing personal information, 16
guidelines, 40
FOI Privacy Officer, 37
in sample policy, 45, 49
must have, 6
Freedom of Information and Protection of Privacy Act, 1, 39

G

Guidelines disclaimer, 2

H

history
of Home Service borrowing, 13
of what a child has borrowed, 12
of what a patron has borrowed, 12, 29
of who borrowed a resource, 13, 29
Home Service
borrowing history, 13
collecting personal information, 8
need certain information, 14
how long to keep personal information, 28
how personal information is used
in sample policy, 47

I

identification, 5
best practices, 5
for debt collection, 5
leaving as collateral, 22
tips for collecting, 6
Information Policy & Privacy Branch
contact information, 39
interlibrary loans, 28

J

janitorial or other services, 31

L

legislation protecting personal information, 1
Library Act, 4
library computers
access to, 18
cache and history folders, 20
destroying computer data, 21
destroying logs, sign-up sheets or registration forms, 20
log of users, 19
registration form, 20
sign-up sheets, 20
surveillance, 21
library referrals, 23
library website
reference questions, 22
links to sites outside of the library
in sample policy, 44

M

marketing or fundraising, 9

N

non-resident privileges, 9
notice
when using computers, 18

O

objectionable behaviour of patrons, 28, 34
Office of the Information and Privacy Commissioner
contact information, 39
Office of the Privacy Commissioner of Canada
contact information, 40
OIPC. *See Office of the Information and Privacy Commissioner*
opt-in, 9
opt-out, 9
other libraries
black lists, 16, 28
debt collection, 16
disclosure of personal information, 27
outside databases, 18
outside service providers, 29
reference questions, 23

P

paper book cards, 14
patron cards
  holding in library, 14
personal identification numbers (PINs), 5
Personal Information Directory (PID), 38
  when new system or changes, 34
Personal Information Protection Act, 2, 39
Personal Information Protection and Electronic Documents Act, 2, 39
personal references
  tips for collecting, 6
PIPA. *See Personal Information Protection Act*
PIPEDA. *See Personal Information and Electronic Documents Act*
police, 26
Privacy Act, 2, 39
Privacy Impact Assessment (PIA)
  as part of Personal Information Directory (PID), 38
  for new or system changes, 34
  for reference question system, 23
  for RFID, 17
  for surveillance, 33
  template, 40
  what it is and when to conduct, 38
  where software service provider, 30
privacy policies and procedures, 7, 36
  communicating, 37
  general privacy policy, 37
  instructions on proper procedures, 37
  sample general privacy policy, 46
  sample website privacy policy, 42
  tips for letting patrons know about, 7
  training, 37
  website privacy policy, 37
  what to include, 36
Privacy Protection Schedule (PPS), 30
  template, 40
pseudonyms
  employees and volunteers, 24

R

receipts for borrowed materials, 10
reference materials, 5
reference questions, 21
  chat system, 23
  emailed to library, 22
  on-line, 17, 22
  patrons asking questions in person, 21
  purchased reference system, 23
  referred, 23
referrals to outside websites, 30
registration
  directly into system, 7
  forms, 6
  on-line, 5, 17
registration form
  sample privacy clause, 41
research, 35
retention of personal information
  in sample policy, 44, 48
RFID (Radio Frequency Identification), 16
  guidelines, 40
room rentals, 35

S

sample authority to collect clause, 41
sample clause for un-secure website communication, 41
sample general privacy policy, 46
sample privacy clauses, 41
sample registration privacy clause, 41
sample website privacy policy, 42
school counsellors, 27
security, 31
  in sample policy, 43, 48
  physical protection of personal information, 32
services provided on behalf of a library, 29
sharing personal information
  over the phone, 11
  with patron's friends or family, 11
smaller communities, 4
social workers, 27
software service providers. *See* outside service providers
statistical purposes, 4
storage or access outside Canada, 33
surveillance
  employees and volunteers, 24
  library computers, 21
  what to consider, 33

T

technological safeguards, 32
training, 37
types of organizations
  federal government institutions, 2
  federally regulated organizations, 2
  local public bodies, 1
  private organizations, 2

U

unreturned materials
  collecting, 14
  collecting ID numbers and reference, 5
  retention of information, 15
using another patron's library card, 11

W

web forms
  in sample policy, 43
website communication un-secure
  sample privacy clause, 41

BRITISH
COLUMBIA

Ministry of Education

Public Library Services Branch